Andere Logiken

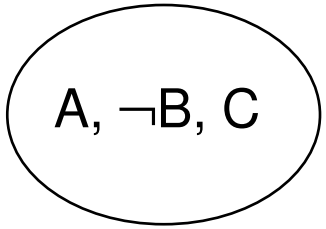
- **Modallogik(en) allgemein**
  Modaloperatoren, Kripke-Semantik, Semantik-Theoreme, Rahmeneigenschaften und Axiome
- **Temporallogik(en)**
  Quantitative Zeitlogiken, PLTL-Operatoren, PLTL-Semantik, Büchi-Automaten, Entscheidbarkeit, ω-reguläre Sprachen
- **Beschreibungslogik(en)**
  Konzepte und Rollen, Entscheidbarkeit

Andere Logiken

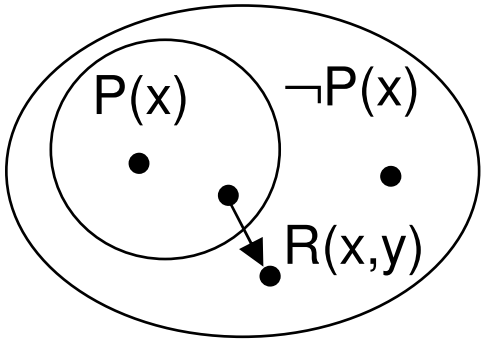
- **Modallogik(en) allgemein**
  - Modaloperatoren
  - Kripke-Semantik
  - Semantik-Theoreme
  - Rahmeneigenschaften und Axiome
- **Temporallogik(en)**
- **Beschreibungslogik(en)**

Fragen und Interpretationen – von der Aussagenlogik bis zur Modallogik

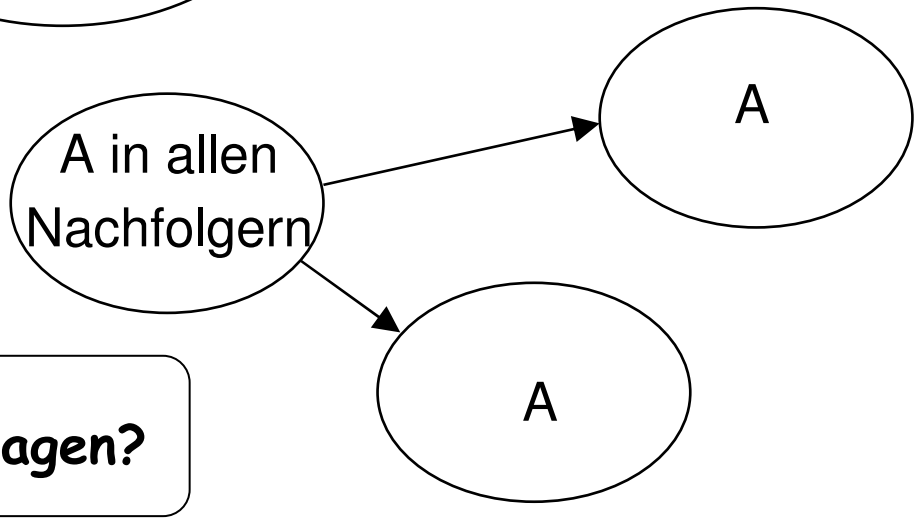
Aussagenlogik:
Was gilt in **einer** (ganzen)
Welt oder **Situation**?



Prädikatenlogik:
Was gilt **für welche Objekte**
in **einer** Welt/**Situation**?



Modallogik (Typ AL):
Was gilt für **welche** (ganzen)
Welten/**Situationen** – auch in
Bezug auf **Übergänge** dazwischen?



Wonach könnte eine weitere Logik fragen?

Modale Logik/Modallogik

Klassische Modallogiken über der Aussagenlogik
verwenden neben den Sprachmitteln der AL
zwei zusätzliche einstellige Operatoren,

$\Box$ (Box) und $\Diamond$ (Karo, Diamond) .

Es gibt auch Modallogik über PL1; diese behandeln wir hier nicht.

Durch

- unterschiedliche praktische Interpretationen … *und daraus resultierend*
- unterschiedliche Axiome … *und evtl.*
- unterschiedliche Ableitungsregeln

ergeben sich **verschiedene Modallogiken**.

Klassische Modallogik(en)

$\Box$ – Es ist **notwendig**, dass ...

$\Diamond$ – Es ist **möglich**, dass ...

Klammerung/Nichtklammerung wie bei $\neg$ → Formelmenge ***MLForm***

Dazu werden generell noch 2 Äquivalenzen gefordert:

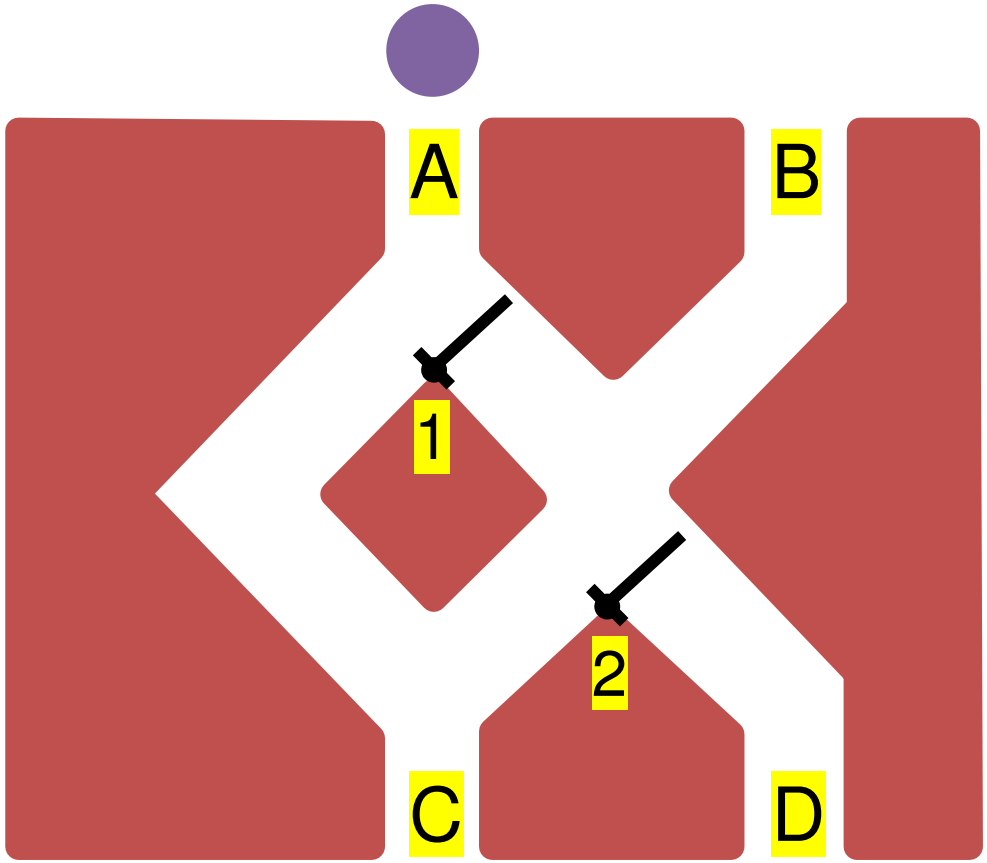
$$\Diamond A \equiv \neg \Box \neg A$$
$$\Box A \equiv \neg \Diamond \neg A$$

Dualität zwischen $\Box$ und $\Diamond$

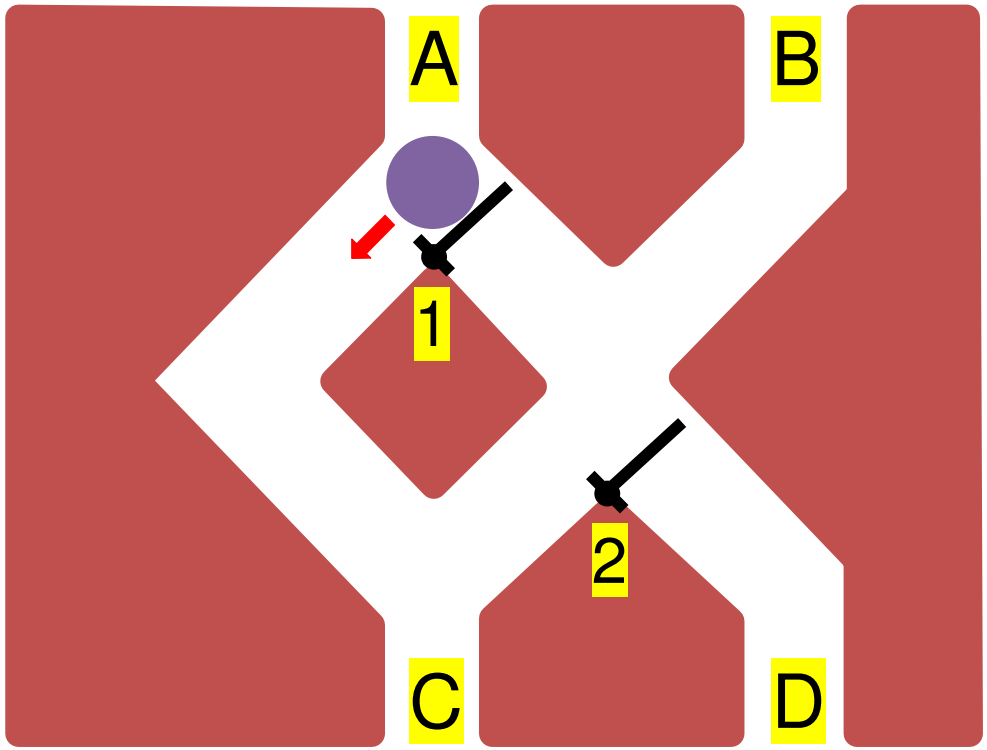
Je nach (philosophischem oder mathematischem) **Notwendigkeitsbegriff** kommen unterschiedliche weitere Axiome hinzu.

→ unterschiedliche klassische modale „Logiken“ (Theorien)

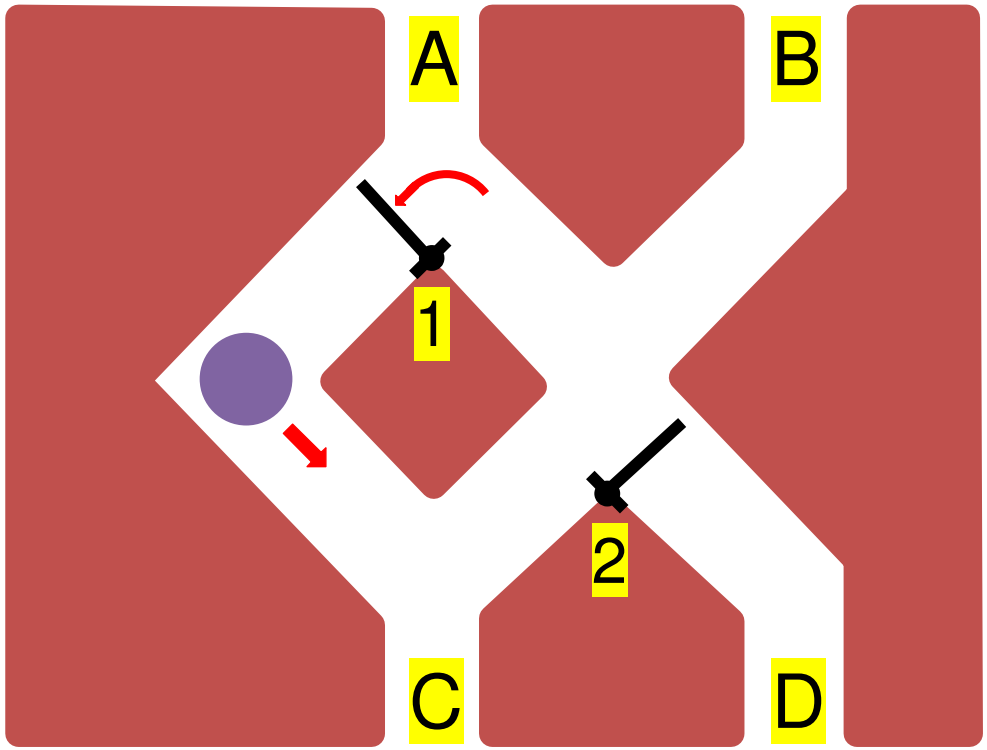
Brettspiel



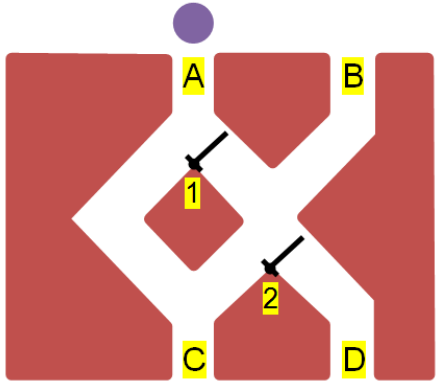
Brettspiel

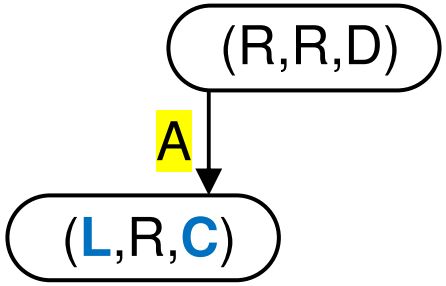


Brettspiel



Brettspiel: Veränderungen





Für die Anfangssituation, d.h.

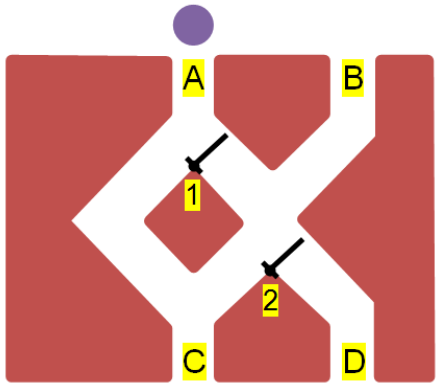
- 1. und 2. Klappe rechts,
- letzte Kugel war durch D herausgekommen ← wieso?

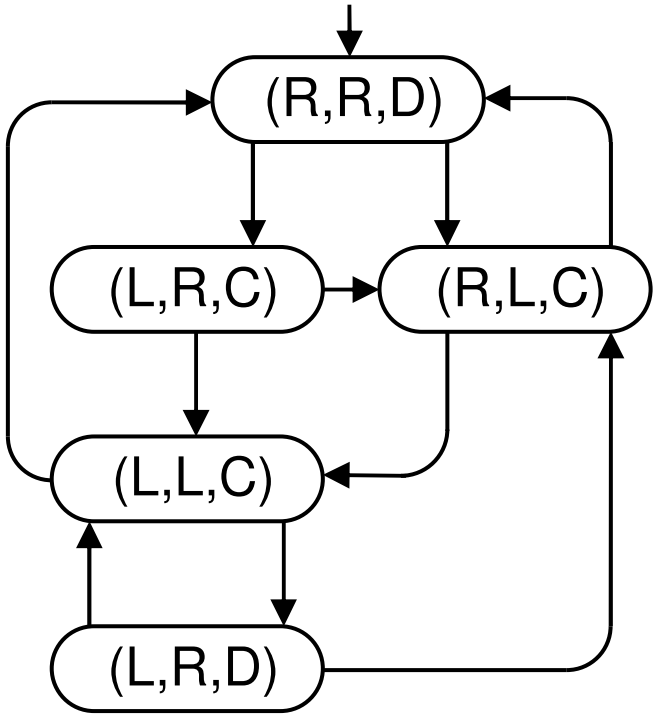
gilt:

Die in A eingeworfene Kugel verändert die Situation:

- **Sie legt Klappe 1 um – von R nach L –**
- **und kommt durch C heraus.**

Brettspiel: alle Möglichkeiten & Fragen





notwendig:
nach der nächsten Kugel muss …

möglich:
nach der nächsten Kugel kann …

Einige Fragen:

- „Wann“ muss die nächste Kugel notwendig nach C? z.B. RRD ⊨ □C
- „Wann“ ist es möglich, eine Kugel so einzuwerfen, dass die folgende Kugel notwendig nach D muss? z.B. RLC ⊨ ◊□D
- Können in der Ausgangssituation zwei Kugeln so eingeworfen werden, dass die folgende Kugel notwendig nach D muss? Ja, RRD ⊨ ◊◊□D

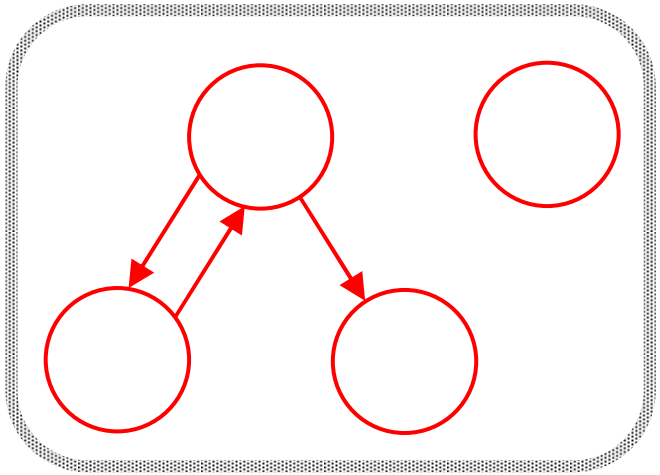
Formale Semantik modaler Logiken
Kripke-Modelle

Kripke-Interpretation (leider auch **„Kripke-Modell“**) $M = (Rah, Bel, Anf)$
(über einer Aussagevariablenmenge AV):
besteht aus: a) Rahmen
b) Belegung
meist auch c) Anfangssituation

a) **(Kripke-) Rahmen** $Rah = (K, R)$ – (gerichteter) **Graph** mit

- der **Knotenmenge** $K \neq \emptyset$ (**„Welten“** oder **„Situationen“**)
- der **Übergangsrelation** $R \subseteq K \times K$ abgebildet als Kanten des Graphen

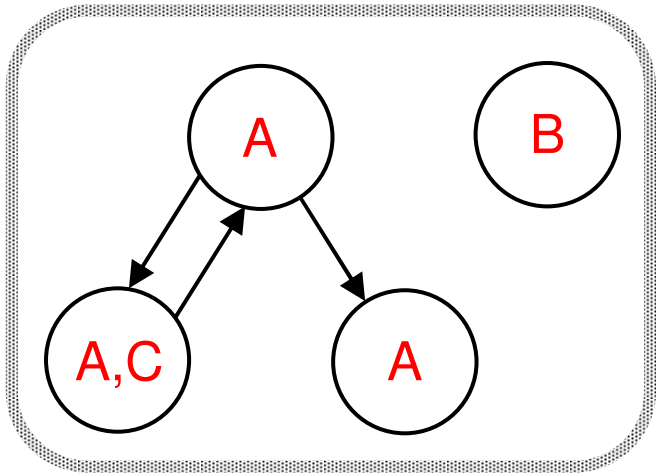
Rahmen-Beispiel:



Kripke-Modelle (2)

b) **Belegung** $Bel : K \rightarrow \mathbf{P}(AV)$ – **Knoteninschrift**-Abbildung

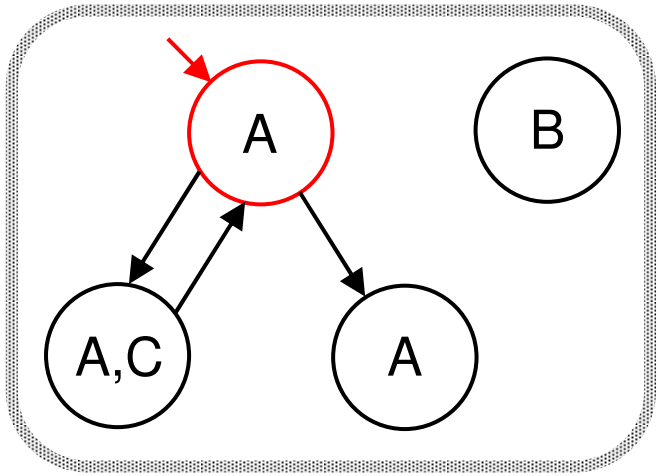
Rahmen+**Belegung**
= **Kripke-Struktur**
Beispiel:



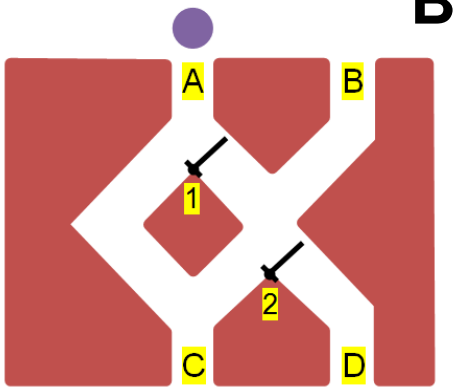
eingetragen:
die mit W belegten
Aussagevariablen

c) **Anfangssituation** $Anf \in K$ – ausgezeichneter **Knoten**

Rahmen+Belegung+
Anfangssituation
Beispiel:



Brettspiel als Kripke-Interpretation

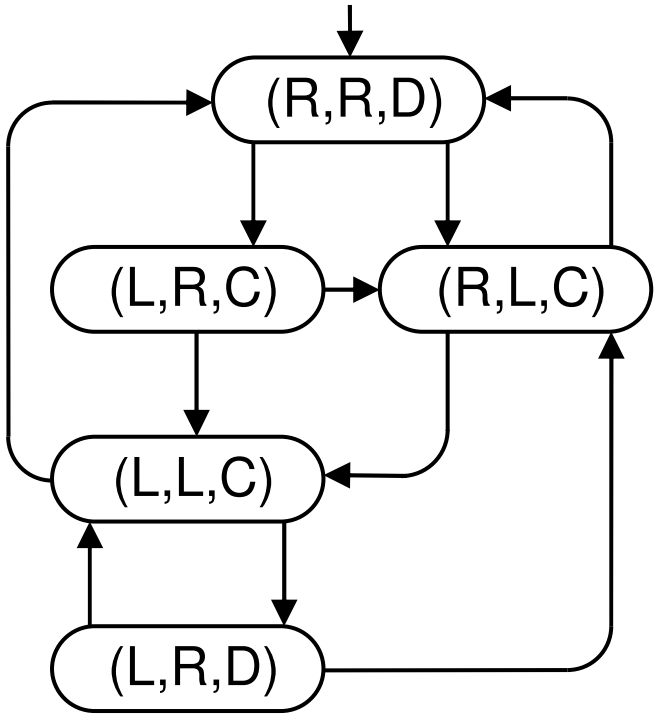


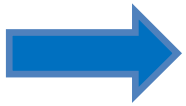
Aussagevariablen

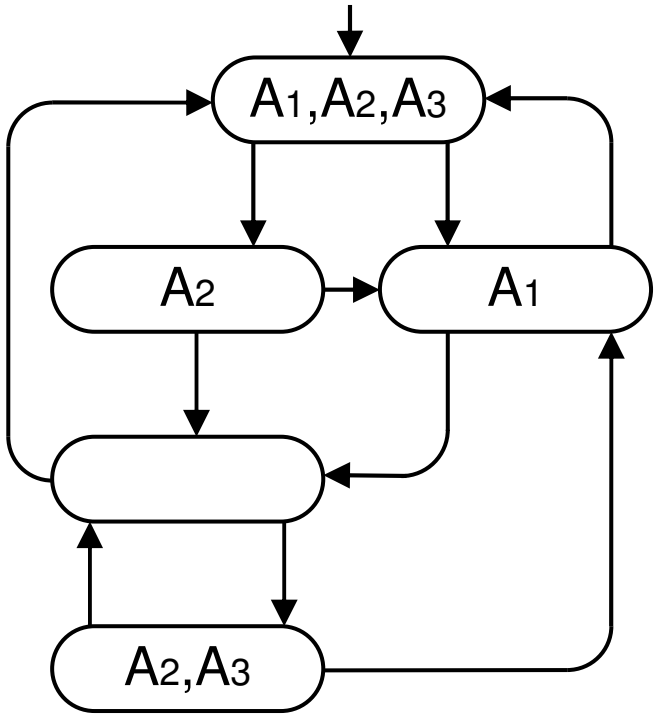
A_1: Klappe 1 rechts

A_2: Klappe 2 rechts

A_3: letzte Kugel bei D







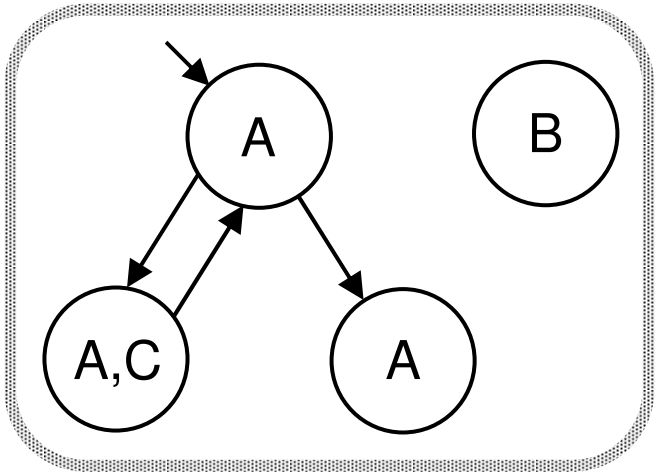
Was ist übrigens mit { A_3 }, { A_1, A_2 }, { A_1, A_3 } ?

Kripke-Semantik: notwendig/möglich

- Von allen **Aussagevariablen** sollen „in der Situation *s*“ genau die dem Knoten *s* zugeordneten A_i aus $\boxed{Bel(s)}$ **wahr** sein.
- **Ohne Modaloperatoren** „geht es nur um die Anfangssituation“ *Anf*.

Jetzt $\Box$(notwendig) und $\Diamond$(möglich) zusätzlich zur AL:

- **Notwendig** sind die Formeln, die **in allen** von *Anf* aus **unmittelbar über 1 Kante erreichbaren** Situationen **wahr** sind:
- **Möglich** sind die Formeln, die **in mindestens einer** von *Anf* aus **unmittelbar über 1 Kante erreichbaren** Situation **wahr** sind.



Im Beispiel und ohne formale Def. …

Intuitiv wahr in $M = (Rah, Bel, Anf)$:
$A, \neg B, \neg C, \Box A, \Diamond C$

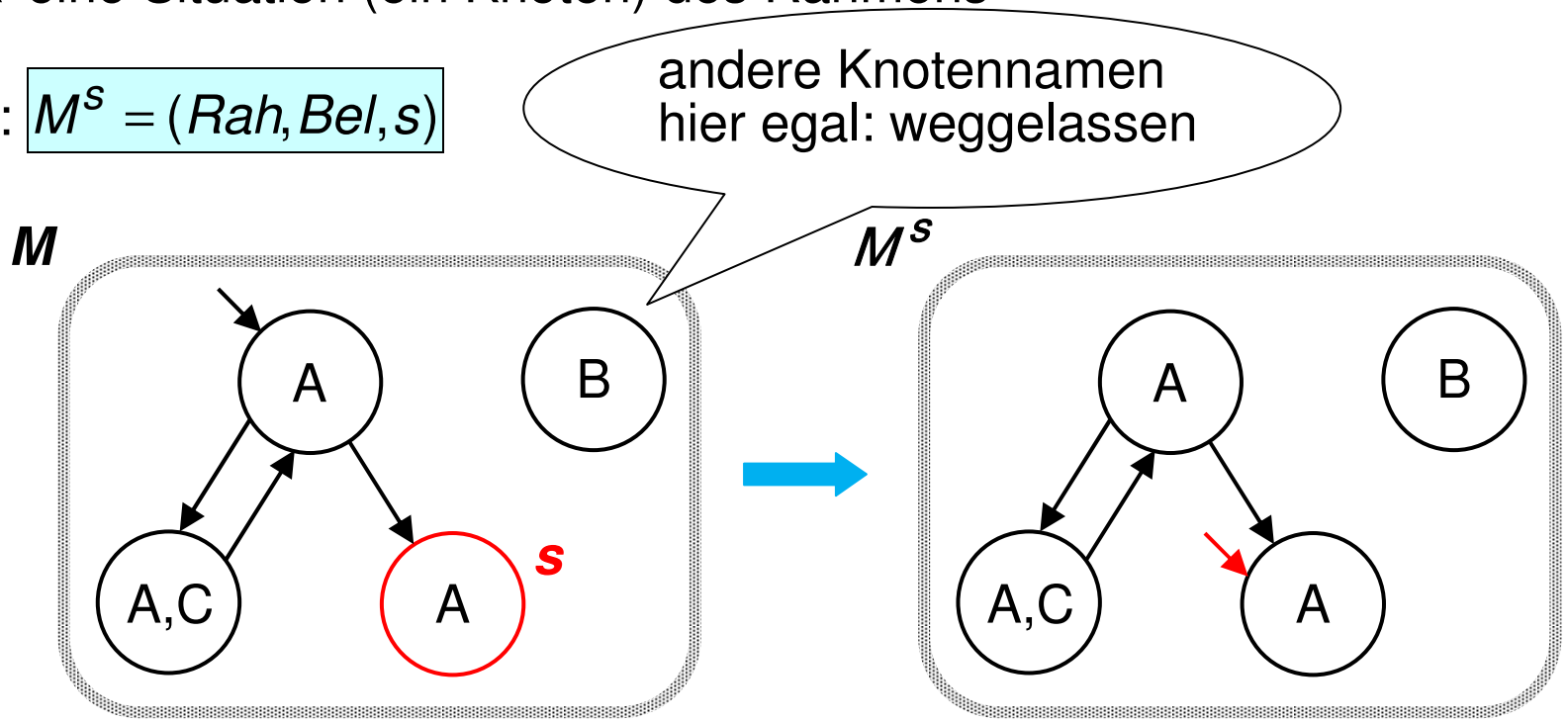
Weniger offensichtlich z.B.:
Gilt $((\Box(A \wedge C)) \rightarrow \Diamond\Diamond \neg C) \rightarrow B$?

Kripke-Semantik – formal
Minidefinition: Übergang zu anderer Anfangssituation

Sei $M = (Rah, Bel, Anf)$ mit $Rah = (K, R)$ eine Kripke-Interpretation und $s \in K$ eine Situation (ein Knoten) des Rahmens

Definition: $M^s = (Rah, Bel, s)$

Beispiel:



→ Natürlich ist $M^{Anf} = M$ und $(M^{s1})^{s2} = M^{s2}$.

Die Definition ist auch gut für $M = (Rah, Bel)$

Kripke-Semantik: Wahrheitswert

Wir definieren den **Wahrheitswert** $wert_M(\varphi)$ einer Modalformel φ in einer Kripke-Interpretation $M = (Rah, Bel, Anf)$ **rekursiv** über den **induktiven Formelaufbau**:

$wert_M\ \varphi$ ist wie folgt definiert:

$\varphi = A_i \in AV \quad \Rightarrow$

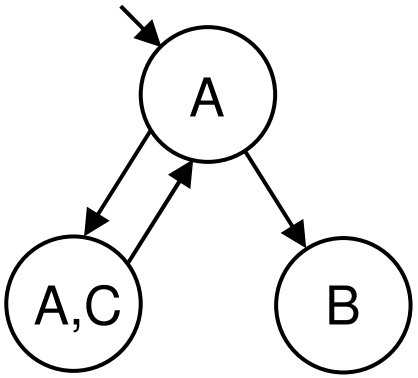
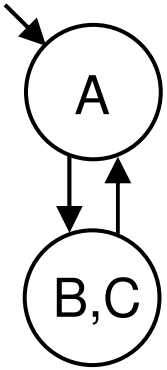
- $wert_M(A_i) :=$ if $A_i \in Bel(Anf)$ then W else F

$\varphi, \psi \in MLForm \ \Rightarrow$

- $wert_M(\neg\varphi) :=$ if $wert_M(\varphi) = W$ then F else W
- $wert_M(\varphi \wedge \psi) :=$ if $wert_M(\varphi) = wert_M(\psi) = W$ then W else F
- $wert_M(\Box\varphi) :=$ if $\forall s \in K : (Anf\ R\ s \Rightarrow wert_M s(\varphi) = W)$ then W else F
- $wert_M(\Diamond\varphi) :=$ if $\exists s \in K : (Anf\ R\ s \wedge wert_M s(\varphi) = W)$ then W else F

$M \models \varphi \ :\Leftrightarrow\ \varphi$ **gilt in** $M \ :\Leftrightarrow\ M$ **erfüllt** / **ist Modell für** $\varphi \ :\Leftrightarrow\ wert_M(\varphi) = W$

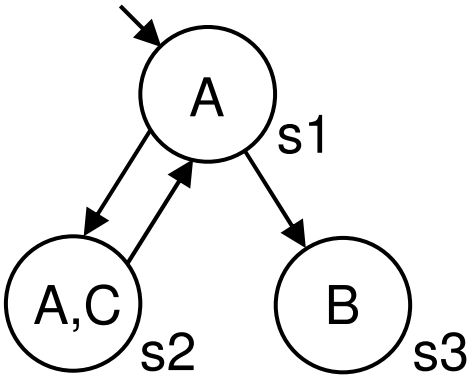
Kripke-Semantik – weitere Beispiele über *A,B,C*

	$\Box\Diamond A$	$\Box(B \rightarrow \neg\Diamond A)$	$\Box(A \rightarrow \Diamond C)$
	F	W	F
	W	F	W

➔ schrittweise „bottom up“ und „über (fast) alle Knoten“

E13

Eine Modallogische Wahrheitstafel 1



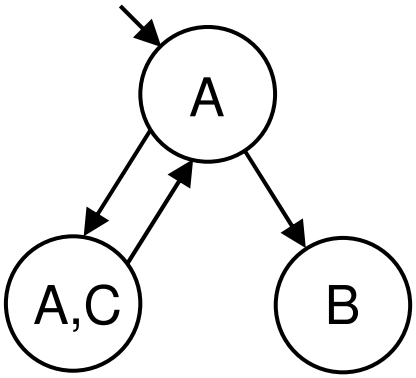
Gibt das Bild wieder.

Formel	**s1** >s2,s3	**s2** >s1	**s3**
A	W	W	F
B	F	F	W
◇A			
¬◇A			
B→¬◇A			
□(B→¬◇A)			

Beispiel
Steht A in s2 oder s3?
→ W

Danach ist gefragt.

Eine Modallogische Wahrheitstafel 2



Gibt das Bild wieder.

Formel	**s1** >s2,s3	**s2** >s1	**s3**
A	W	W	F
B	F	F	W
◇A	W	W	F
¬◇A	F	F	W
B→¬◇A	W	W	W
□(B→¬◇A)	W	W	W

Danach war gefragt.

Ü40

Kripke-Semantik: Gültigkeit auf anderen Ebenen

Manchmal interessiert, ob eine Formel in einer **Kripke-Struktur** (Rah, Bel) **in jeder möglichen Situation** wahr ist:

$(Rah, Bel) \models \varphi$

$:\Leftrightarrow (Rah, Bel)$ **erfüllt / ist Modell für** φ, φ **gilt in** (Rah, Bel)
$:\Leftrightarrow \forall s \in K : (Rah, Bel, s) \models \varphi$

Manchmal interessiert, ob eine Formel in einem **Rahmen sogar bei jeder möglichen Belegung und in jeder möglichen Situation wahr** ist:

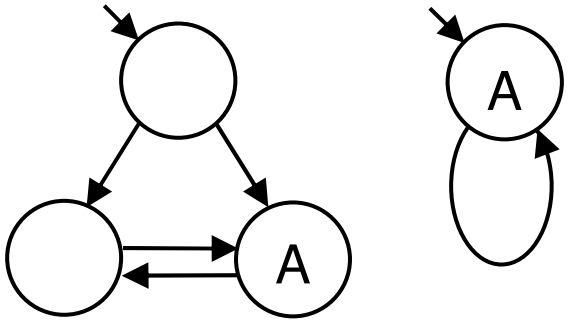
$Rah \models \varphi$

$:\Leftrightarrow Rah$ **erfüllt / ist Modell für** φ, φ **gilt in** Rah
$:\Leftrightarrow \forall \text{Abb}. Bel : K \to P(AV) : (Rah, Bel) \models \varphi$
$:\Leftrightarrow \forall \text{Abb}. Bel : K \to P(AV) : \forall s \in K : (Rah, Bel, s) \models \varphi$

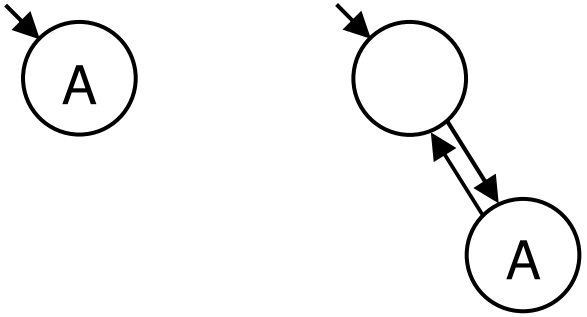
→ nur noch Eigenschaften der Relation/ des Graphen.

Modelle und Gegenbeispiele für $\Diamond\Box A$

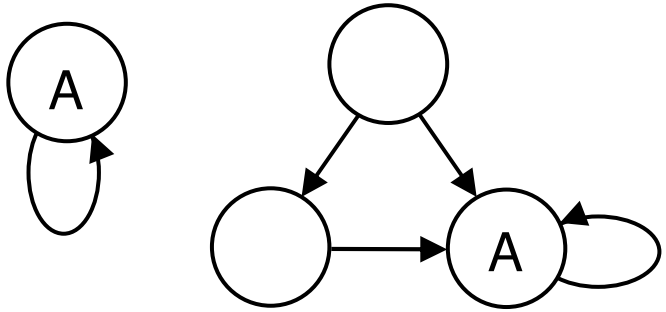
Modelle mit Anf.-Situation



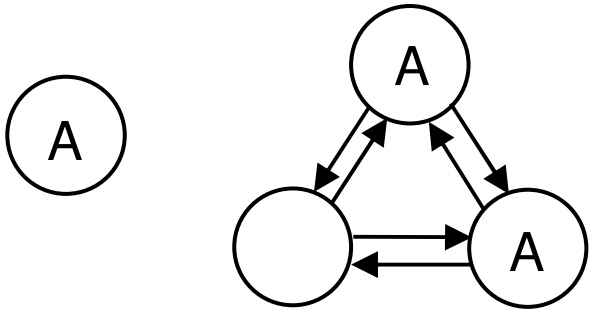
Gegenbsp. mit Anf.-Situation



Kripke-Struktur-Modelle



Kripke-Struktur-Gegenbsp.



Rahmen-Modelle

keine!

höchstens bzgl. Rahmen mit Anf.-Sit.

Rahmen-Gegenbsp.

alle

Wieso gilt in keinem Kripke-Rahmen $\Diamond\Box A$?

Annahme (#): Es existiert ein Rahmen *Rah* mit $\Diamond\Box A$
für alle Belegungen und alle Wahlen der Anfangssituation.

Belege (*Bel*) alle Knoten *K* leer, so dass überall $\neg A$ gilt.

$\Rightarrow$ (*) Jeder Knoten, in dem $\Box A$ gilt, hat keine Nachfolger
(*sonst gälte im Nachfolger A und (s.o.)* $\neg A$)

Sei K_A Anfangsknoten in *Rah* mit Belegung *Bel*,

$\Rightarrow$ In K_A gilt $\Diamond\Box A$ – wegen (#)

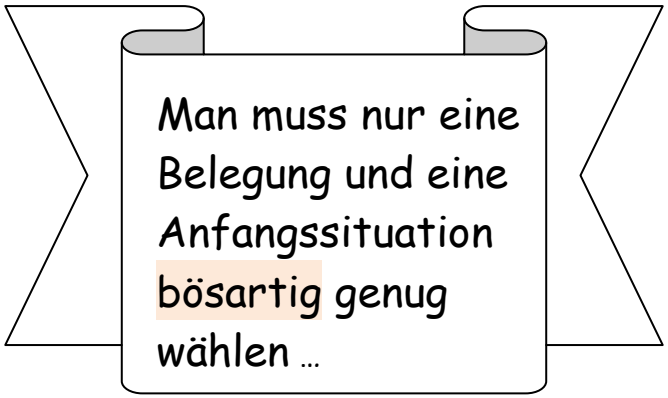
$\Rightarrow$ K_A hat Nachfolgerknoten *L*, in dem $\Box$A gilt.

$\Rightarrow$ *L* hat keine Nachfolger – wegen (*)

Sei nun *L* Anfangsknoten in *Rah* mit Belegung *Bel*

$\Rightarrow$ In *L* gilt $\Diamond\Box A$ – wegen (#)

$\Rightarrow$ *L* hat Nachfolger, ↯



Aquivalenz, Tautologien, Erfüllbarkeit

Äquivalent ($\equiv$) sind ML-Formeln, die genau die **gleichen (erfüllenden) Kripke-Modelle** (Rah, Bel, Anf) haben.

Beispiele: $\Box(A \wedge B) \equiv (\Box A \wedge \Box B)$, $\Diamond \neg A \equiv \neg \Box A$

Allgemeingültig (ML-Tautologien, MLT) sind ML-Formeln, die **in allen Kripke-Interpretationen** (Rah, Bel, Anf) gelten,

z.B. $\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$ (**K**), $\Diamond(A \vee B) \leftrightarrow (\Diamond A \vee \Diamond B)$

Erfüllbar sind ML-Formeln, die **mindestens ein (erfüllendes) Kripke-Modell** (Rah, Bel, Anf) haben. Sonst sind sie unerfüllbar.

Substitution, Ersetzung, Normalform

Man kann …

- in einer **tautologischen AL-Formel alle Vorkommen** einer Aussagevariable durch dieselbe ML-Formel ersetzen, und man erhält eine **ML-Tautologie** (**Substitutionslemma**);
- in einer ML-Formel φ **ein Vorkommen einer Teilformel** durch eine dazu **äquivalente ML-Formel** ersetzen, und man erhält eine **zu φ äquivalente ML-Formel** (**Ersetzungslemma**);
- eine zu einer gegebenen ML-Formel eine äquivalente ML-Formel konstruieren, bei der alle **Negationen unmittelbar vor Aussagevariablen** stehen – eine **Normalform**.

Ein ML-Kalkül

Die …

- AL-Axiome, AL-Ableitungsregeln (also alle **AL-Tautologien**)
- **Substitution** und **Ersetzung** in MLT's,
- die 2 **ML-Axiome**: (K) und $\Box A \leftrightarrow \neg\Diamond\neg A$,
- **Notwendigkeit** der ML-Tautologien: φ MLT $\Rightarrow \Box\varphi$ MLT,
- **ML-Modus-Ponens**: φ und $\varphi\rightarrow\psi$ MLT'en $\Rightarrow$ ψ MLT,

bilden einen korrekten und vollständigen **Kalkül** zur Ableitung von ML-Tautologien.

Man kann auch den **Werkzeugkasten** um ML-Regeln (u.a.) erweitern.

Spezielle Rahmen in Kripke-Semantiken

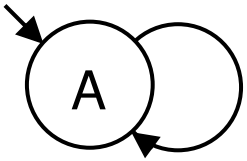
Besondere **Graphen/Relationen-Eigenschaften** der Rahmen	⟺	Einführung besonderer **Axiome** der zugehörigen modalen Logik.

- Graph festhalten, Belegung und Anfangssituation dürfen **variieren**.
- Welche Eigenschaft muss der Graph haben, damit **stets** das Axiom gilt?
- Welche Axiome gelten bei gegebener Grapheneigenschaft?

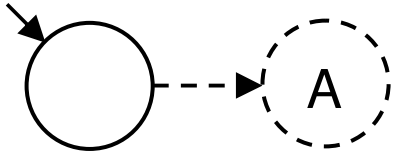
Beispiele

R reflexiv $\Leftrightarrow$ $\Box A \rightarrow A$

li. $\Rightarrow$ *re.* : Ist *R* reflexiv und A notwendig, so gilt *Anf R Anf* und $\Box A$, also gilt *A* in *Anf*.



$\neg$ *li.* $\Rightarrow$ $\neg$ *re.* („*sonst*“): Ist *R* nicht reflexiv, so existiert ein Knoten k mit $\neg kRk$. Mache *k* zu *Anf* und belege alle Nachfolger von *k* mit *A*, *k* aber nicht: $\Box A \wedge \neg A$)

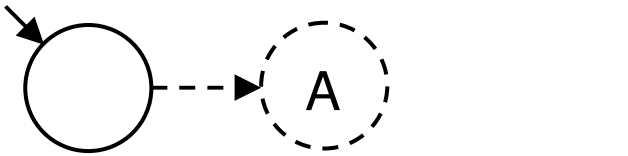
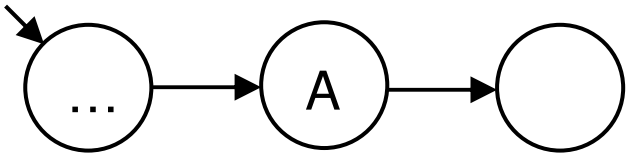


Spezielle Rahmen in Kripke-Semantiken

Besondere **Graphen/Relationen-Eigenschaften** der Rahmen	⟺	Einführung besonderer **Axiome** der zugehörigen modalen Logik.

- Graph festhalten, Belegung und Anfangssituation dürfen **variieren**.
- Welche Eigenschaft muss der Graph haben, damit **stets** das Axiom gilt?
- Welche Axiome gelten bei gegebener Grapheneigenschaft?

Beispiele

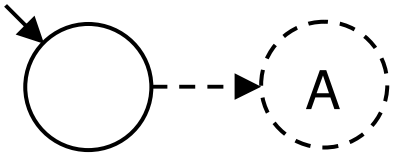
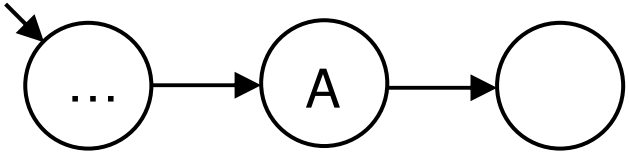
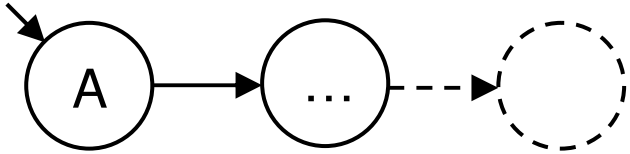
R reflexiv	–	$\Box A \rightarrow A$	*sonst:*	
R transitiv	–	$\Box A \rightarrow \Box\Box A$	*sonst:*	
***R* symmetrisch**	–	**???**		
R **???**	–	$\Box A \rightarrow \Diamond A$		

Spezielle Rahmen in Kripke-Semantiken

Besondere **Graphen/Relationen-Eigenschaften** der Kripke-Modelle	⟺	Einführung besonderer **Axiome** der zugehörigen modalen Logik.

- Graph festhalten, Belegung und Anfangssituation dürfen **variieren**.
- Welche Eigenschaft muss der Graph haben, damit **stets** das Axiom gilt?
- Welche Axiome gelten bei gegebener Grapheneigenschaft?

Beispiele

R reflexiv	–	$\Box A \rightarrow A$	*sonst:*	
R transitiv	–	$\Box A \rightarrow \Box\Box A$	*sonst:*	
R **symmetrisch**	–	$A \rightarrow \Box\Diamond A$	*sonst:*	
R **???**	–	$\Box A \rightarrow \Diamond A$		

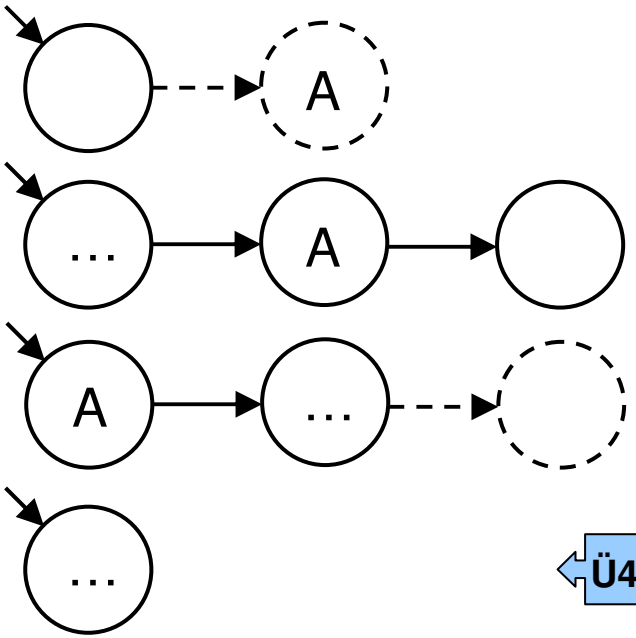
Spezielle Rahmen in Kripke-Semantiken

Besondere **Graphen/Relationen-Eigenschaften** der Kripke-Modelle	⟺	Einführung besonderer **Axiome** der zugehörigen modalen Logik.

- Graph festhalten, Belegung und Anfangssituation dürfen **variieren**.
- Welche Eigenschaft muss der Graph haben, damit **stets** das Axiom gilt?
- Welche Axiome gelten bei gegebener Grapheneigenschaft?

Beispiele

R reflexiv	–	$\Box A \rightarrow A$	*sonst:*
R transitiv	–	$\Box A \rightarrow \Box\Box A$	*sonst:*
R symmetrisch	–	$A \rightarrow \Box\Diamond A$	*sonst:*
***R* linkstotal**	–	$\Box A \rightarrow \Diamond A$	*sonst:*



Ü41

Beispiel einer Modallogik: Situationenmenge (1)

Man arbeitet mit einer gegebenen **Menge**

MB möglicher **Belegungen** von $A_1, \ldots, A_n$.

Mit

- Knotenmenge *MB* (Situationen = Belegungen)
- *bel* = id_{MB} (Situationen = Belegungen)
- Relation $MB \times MB$ (totale Äquivalenzrelation, d.h. alle Situationen in *MB* sind stets in 1 Schritt erreichbar.)
- Anfangsknoten $Anf \in MB$ (beliebig)

⇨ Dann bedeutet <u>für AL-Formeln</u>:

notwendig :⇔ in allen Situationen/Belegungen aus *MB*

möglich :⇔ in mindestens einer Situation/Belegung aus *MB*

⇨ … eine besonders **einfache** Bedeutung von **notwendig** und **möglich**.

Beispiel einer Modallogik: Situationenmenge (2)

Spezialfall:

- Man betrachtet nur AL-Formeln.
- *MB* = Menge **aller** totalen Belegungen

Dann bedeutet für AL-Formeln:

notwendig	⇔	**allgemeingültig (in AL)**
möglich	⇔	**erfüllbar (in AL)**

Hier sind semantische Begriffe der AL syntaktisch **innerhalb** einer modalen Logik ausdrückbar.

Beispiel einer Modallogik: Deontische Logik

$\Box$ – Es ist **geboten** (Pflicht), dass ...

$\Diamond$ – Es ist **erlaubt**, dass ...

Nachvollziehbare **Axiome**, z.B.:

$$\Diamond A \leftrightarrow \neg \Box \neg A$$

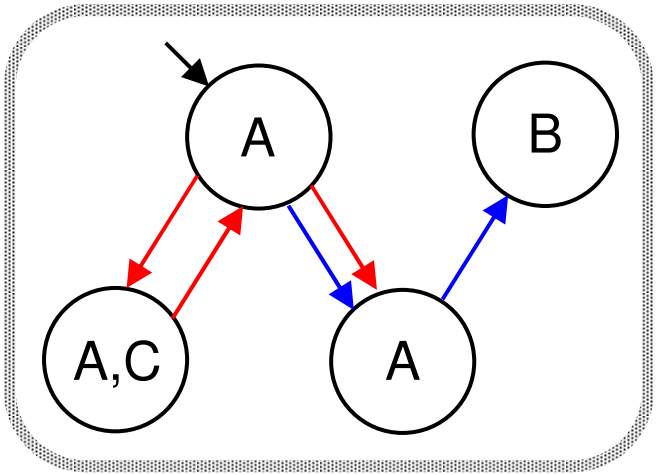
Zusammenhänge mit **juristischem Denken**.

Andere **angewandte Modallogiken** haben ihre
eigenen praktisch motivierten Axiome →

normative, alethische, epistemische, doxastische,
intensionale, dynamische, temporale Logik

Allgemeinere Formen der Modallogik

In manchen Fragen ist es sinnvoll mehrere unterschiedliche Übergangsrelationen zwischen den Welten gleichzeitig zu betrachten:



Entsprechend gibt es dann unterschiedliche Möglichkeits- und Notwendigkeits-operatoren: $\Box$, $\Box$, $\Diamond$, $\Diamond$

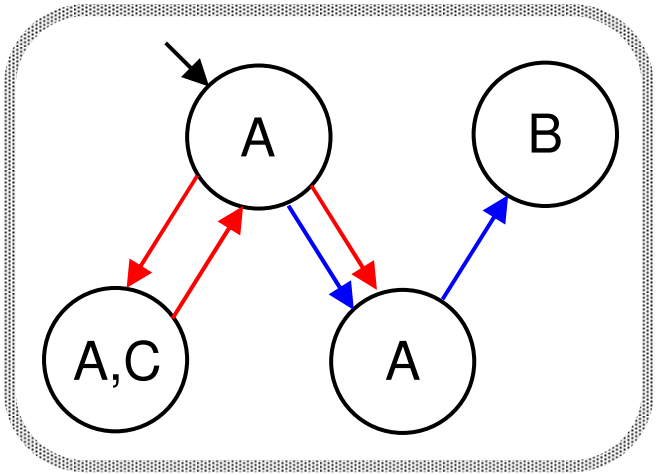
Häufig spricht man von Relationen R_1, R_2, R_3, ... und schreibt die zugehörigen Modaloperatoren als $[1]$, $[2]$, ..., $\langle 1 \rangle$, $\langle 2 \rangle$, ...

→ Multimodale Logiken

Hatten wir schon ein konkretes Beispiel?

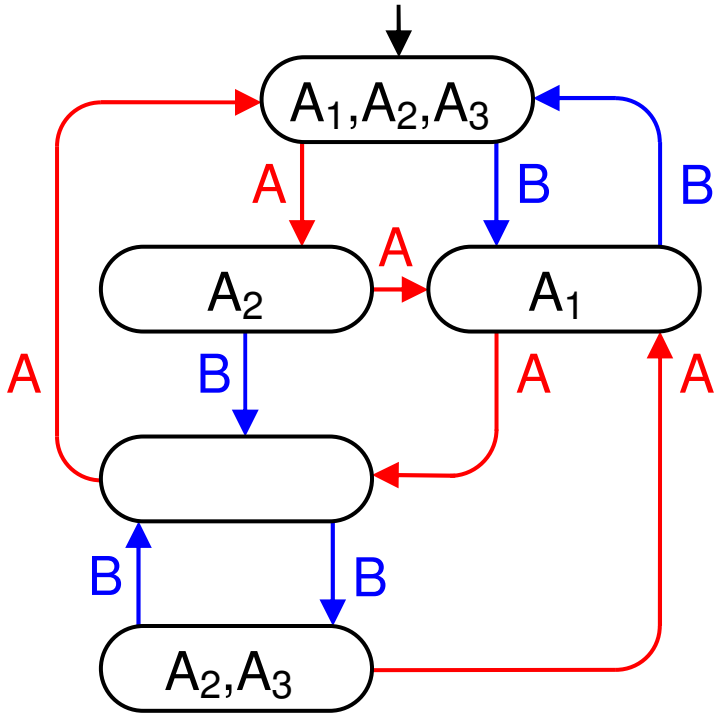
Allgemeinere Formen der Modallogik

In manchen Fragen ist es sinnvoll mehrere unterschiedliche Übergangsrelationen zwischen den Welten gleichzeitig zu betrachten:



Entsprechend gibt es dann unterschiedliche Möglichkeits- und Notwendigkeits-operatoren: $\Box$, $\Box$, $\Diamond$, $\Diamond$

Häufig spricht man von Relationen R_1, R_2, R_3, ... und schreibt die zugehörigen Modaloperatoren als $[1]$, $[2]$, ..., $\langle 1 \rangle$, $\langle 2 \rangle$, ...



→ Multimodale Logiken

Hatten wir schon ein konkretes Beispiel?

Ja

Andere Logiken

- Modallogik(en)
- **Temporallogik(en)**
  - Quantitative Zeitlogiken
  - PLTL-Operatoren
  - PLTL-Semantik
  - Büchi-Automaten
  - Entscheidbarkeit
  - ω-reguläre Sprachen
- Beschreibungslogik(en)

Logiken mit Zeit (1)

Bei Spezifikation und Test realer Systeme möchte man oft

Anforderungen an zeitliche Abläufe

darstellen und behandeln.

Manchmal hat man

- **quantitative** Anforderungen an **Zeiträume** und **Zeitpunkte**,
  - Die Seite muss spätestens 4 Sekunden nach dem Aufruf vollständig auf dem Bildschirm aufgebaut sein.
  - Die Uhr soll zu jeder vollen Stunde schlagen.
  - Der Angestellten sollen jeden Werktag 8 Stunden arbeiten.

Dazu eignen sich z.B.

Zeitnetze (z.B. Timer Nets)
Zeitautomaten (Timed Automata)

Logiken mit Zeit (2)

Manchmal genügt es, dass („qualitativ“) in der **Abfolge** beispielsweise

- etwas Erwünschtes im nächsten Schritt oder zumindest irgendwann oder solange notwendig, bzw.
- etwas Unerwünschtes nie oder höchsten alle *n* mal

der Fall ist.

- Wenn ich die Nachricht immer wieder sende, muss sie irgendwann ankommen.
- Solange ich noch keine Empfangsbestätigung habe, sende ich die Nachricht immer wieder.
- Das Kommunikationsmedium verfälscht keine Nachricht.

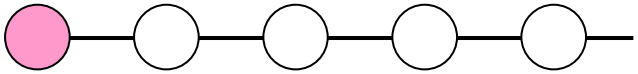
Temporallogik

Lineare Temporale Aussagenlogik, PLTL

Propositional Linear Temporal Logic

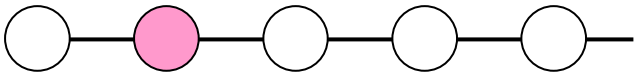
Aussagenlogik

φ anfangs (implizit)



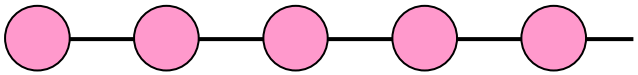
+ **temporale Operatoren** ...

Xφ als Nächstes neXt



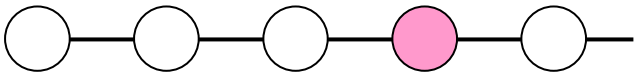
Gφ stets Generally,

always, auch „$\Box$“

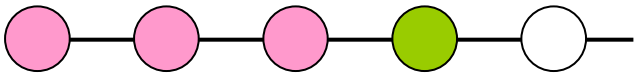


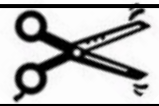
Fφ irgendwann Future,

some time, auch „$\Diamond$“



(φ U ψ) mindestens bis Until



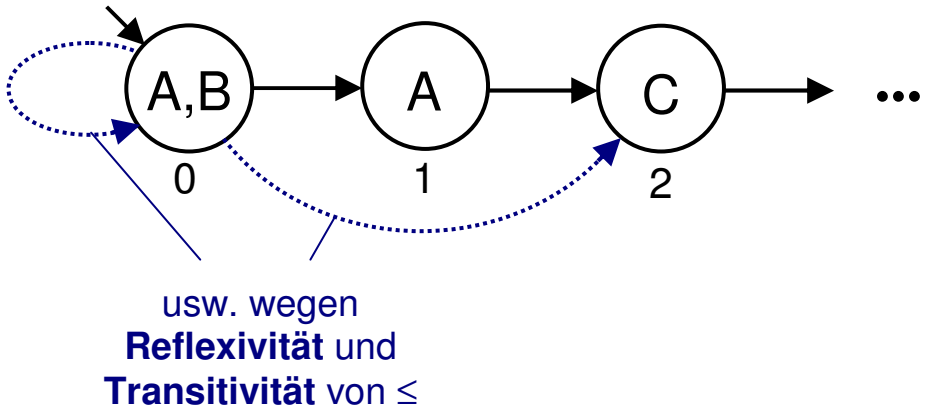
genauer:  -Semantik

intuitiv, vereinfacht!

PLTL als modale Logik

Die potentiellen **Modelle** (Interpretationen) sind unendliche Folgen $\pi = (\pi_0, \pi_1, \ldots)$ von „Gegebenheiten“ (Zuständen, Situationen), in denen jeweils alle Aussagevariablen in einer Menge $\pi_i \subseteq AV$ wahr sind (und die anderen – in $AV \setminus \pi_i$ – nicht).

→ **Kripke-Semantik** mit speziellen Graphen, nämlich isomorph zu $(\mathbb{N}_0, \leq)$:



PLTL-Syntax, formal

Die **Formeln** der PLTL sind induktiv definiert:

- Alle Aussagevariablen in AV sind PLTL-Formeln.
- Für alle PLTL-Formeln φ, ψ sind ebenfalls PLTL-Formeln ...
  - Aussagenlogik
    $(\neg\varphi)$ und $(\varphi \wedge \psi)$ (1)
  - Temporale Logik
    $(\mathrm{X}\,\varphi)$, $(\mathrm{G}\,\varphi)$, $(\mathrm{F}\,\varphi)$ und $(\varphi\,\mathrm{U}\,\psi)$ (2)

△ Achtung!
Viele Texte verwenden auch andere Operatoren bzw. Schreibweisen ...

1) AL-Operatoren oben minimal. $\vee$, $\rightarrow$ und $\leftrightarrow$ kann man mit auflisten oder als expandierbare Abkürzungen behandeln.
2) TempL-Operatoren minimal? → Übung später

Formale PLTL-Semantik (1)

... legt fest,
wann eine PLTL-Formel auf einer Folge $\pi = (\pi_0, \pi_1, \ldots)$, $\pi_i \subseteq AV$, **wahr** ist.

Gültigkeit von Aussagevariablen: im ersten Folgenglied

- Für $\varphi \in AV$: $\pi \models \varphi \;\; :\Leftrightarrow \quad \varphi \in \pi_0$ **gilt im ersten Folgenglied**

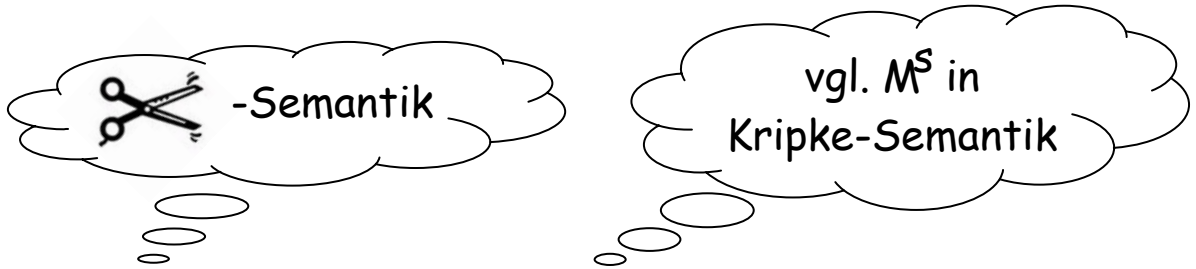
ansonsten für PLTL-Formeln φ, ψ :

Aussagenlogik

- $\pi \models \neg\varphi \quad :\Leftrightarrow$ nicht $\pi \models \varphi$
- $\pi \models \varphi \wedge \psi \;\; :\Leftrightarrow \;\; \pi \models \varphi$ und $\pi \models \psi$
- analog bzw. als Abkürzung: die logischen Operatoren $\vee$, $\rightarrow$, $\leftrightarrow$

Formale PLTL-Semantik (2)

und für PLTL-Formeln φ, ψ:



Temporaler Anteil

- $\pi \models \mathsf{X}\varphi \quad :\Leftrightarrow \quad \pi^1 \models \varphi$ φ gilt im **nächsten** Folgenglied
- $\pi \models \mathsf{G}\varphi \quad :\Leftrightarrow \quad \forall i \geq 0 : \pi^i \models \varphi$ φ gilt in **allen** Folgengliedern
- $\pi \models \mathsf{F}\varphi \quad :\Leftrightarrow \quad \exists i \geq 0 : \pi^i \models \varphi$ φ gilt in **einem** Folgenglied
- $\pi \models \varphi \mathsf{U} \psi \quad :\Leftrightarrow \quad (\exists i \geq 0 : \pi^i \models \psi) \wedge (\forall 0 \leq j < i : \pi^j \models \varphi)$

  ψ gilt in **einem** Folgenglied, und mindestens bis unmittelbar **davor** gilt φ.

Zusammenhänge und weitere Temporaloperatoren

Die Operatoren G und F können **durch U** (und AL) **ausgedrückt** werden:

- $\mathsf{F}\varphi \quad \equiv \quad \mathsf{T}\ \mathsf{U}\ \varphi \quad \equiv \quad (A \vee \neg A)\ \mathsf{U}\ \varphi$
- $\mathsf{G}\varphi \quad \equiv \quad \neg\mathsf{F}\neg\varphi \quad \equiv \quad \neg\,(\mathsf{T}\ \mathsf{U}\ \neg\varphi)$

Einige **weitere Temporaloperatoren**:

- $\varphi\,\mathsf{R}\,\psi$: ψ gilt bis zu und einschließlich dem ersten Folgenglied, an dem φ gilt, sofern ein solches existiert; andernfalls gilt ψ für immer.
- $\varphi\,\mathsf{W}\,\psi$: *W*enn φ nicht für immer gilt, dann mindestens bis unmittelbar vor das – dann sicher kommende – erste Folgenglied, an dem ψ gilt.
- $\mathsf{Op1}\varphi$: φ gilt unendlich oft.
- $\mathsf{Op2}\varphi$: φ gilt unendlich oft nicht.
- $\mathsf{Op3}\varphi$: φ gilt nie.

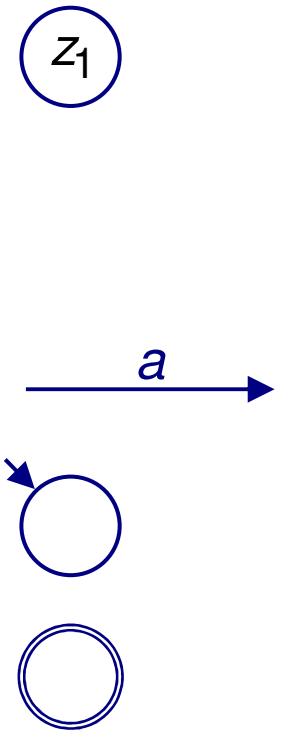
Fingerübung: Operatoren durch andere ausdrücken

Ü42

Automaten

Ein Automat („über Σ“) ist ein Quintupel $A = (Z, \Sigma, T, Z_{Anf}, Z_{Ziel})$ mit

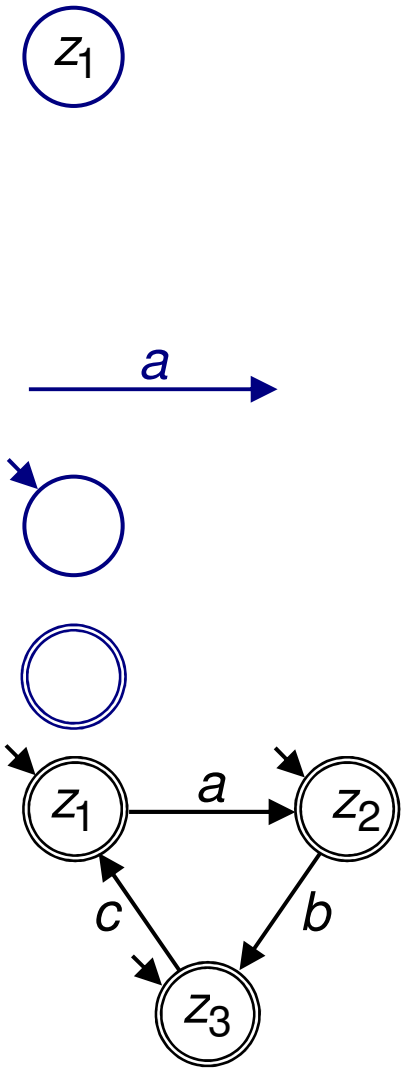
- einer endlichen Menge Z, deren Elemente **Zustände** genannt werden;
- einer endlichen Menge Σ (**Alphabet**), deren Elemente **Symbole** genannt werden;
- einer dreistelligen **Transitions-** (Übergangs-) **Relation** $T \subseteq Z \times \Sigma \times Z$;
- einer Menge $Z_{Anf} \subseteq Z$, deren Elemente **Anfangszustände** genannt werden;
- einer Menge $Z_{Ziel} \subseteq Z$, deren Elemente **Zielzustände** genannt werden.



Automaten

Ein Automat („über Σ“) ist ein Quintupel $A = (Z, \Sigma, T, Z_{Anf}, Z_{Ziel})$ mit

- einer endlichen Menge Z, deren Elemente **Zustände** genannt werden;
- einer endlichen Menge Σ (**Alphabet**), deren Elemente **Symbole** genannt werden;
- einer dreistelligen **Transitions-** (Übergangs-) **Relation** $T \subseteq Z \times \Sigma \times Z$;
- einer Menge $Z_{Anf} \subseteq Z$, deren Elemente **Anfangszustände** genannt werden;
- einer Menge $Z_{Ziel} \subseteq Z$, deren Elemente **Zielzustände** genannt werden.



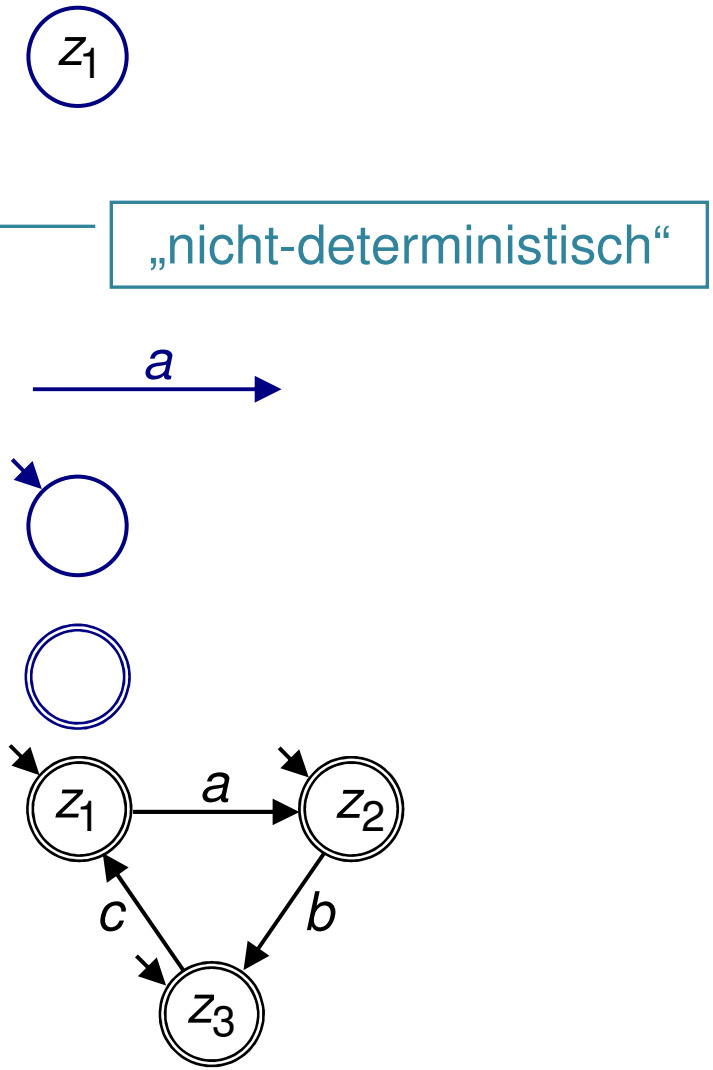
Beispiel

- $Z = Z_{Anf} = Z_{Ziel} = \{z_1, z_2, z_3\}$
- $\Sigma = \{a, b, c\}$
- $T = \{(z_1, a, z_2), (z_2, b, z_3), (z_3, c, z_1)\}$

Automaten

Ein Automat („über Σ“) ist ein Quintupel $A = (Z, \Sigma, T, Z_{Anf}, Z_{Ziel})$ mit

- einer endlichen Menge Z, deren Elemente **Zustände** genannt werden;
- einer endlichen Menge Σ (**Alphabet**), deren Elemente **Symbole** genannt werden;
- einer dreistelligen **Transitions-** (Übergangs-) **Relation** $T \subseteq Z \times \Sigma \times Z$;
- einer Menge $Z_{Anf} \subseteq Z$, deren Elemente **Anfangszustände** genannt werden;
- einer Menge $Z_{Ziel} \subseteq Z$, deren Elemente **Zielzustände** genannt werden.



Beispiel

- $Z = Z_{Anf} = Z_{Ziel} = \{z_1, z_2, z_3\}$
- $\Sigma = \{a, b, c\}$
- $T = \{(z_1, a, z_2), (z_2, b, z_3), (z_3, c, z_1)\}$

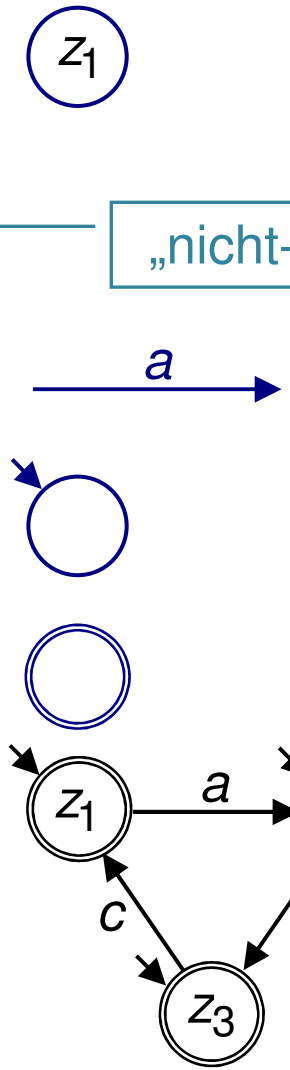
Automaten

Ein Automat („über Σ“) ist ein Qintupel $A = (Z, \Sigma, T, Z_{Anf}, Z_{Ziel})$ mit

- einer endlichen Menge Z, deren Elemente **Zustände** genannt werden;
- einer endlichen Menge Σ (**Alphabet**), deren Elemente **Symbole** genannt werden;
- einer dreistelligen **Transitions-** (Übergangs-) **Relation** $T \subseteq Z \times \Sigma \times Z$;
- einer Menge $Z_{Anf} \subseteq Z$, deren Elemente **Anfangszustände** genannt werden;
- einer Menge $Z_{Ziel} \subseteq Z$, deren Elemente **Zielzustände** genannt werden.

Gleich nicht mehr egal !!

„nicht-deterministisch“



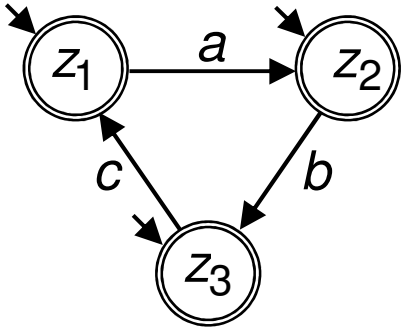
Beispiel

- $Z = Z_{Anf} = Z_{Ziel} = \{z_1, z_2, z_3\}$
- $\Sigma = \{a, b, c\}$
- $T = \{(z_1, a, z_2), (z_2, b, z_3), (z_3, c, z_1)\}$

Automaten und Sprachen

Beispiel

- $Z = Z_{Anf} = Z_{Ziel} = \{z_1, z_2, z_3\}$
- $\Sigma = \{a, b, c\}$
- $T = \{(z_1, a, z_2), (z_2, b, z_3), (z_3, c, z_1)\}$



Ein Automat *A* definiert („**akzeptiert**“) eine **Sprache** L(*A*) (endlicher Wörter) nach dem „Prinzip der **möglichen Reisetagebücher**“:
Wir lassen uns in einem Anfangszustand absetzen, reisen entlang der Pfeile von Zustand zu Zustand und schreiben dabei die Pfeilanschriften mit. In jedem Endzustand dürfen wir aufhören, müssen aber nicht. Was wir bis dahin mitgeschrieben haben, ist ein Wort der Sprache.

– Formale Definition? –

oben:

$$\begin{aligned} L(A) &= \{\varepsilon, a, b, c, ab, bc, ca, abc, bca, \ldots\} \\ &= \text{Pref}(\text{Suff}((abc)^*)) \\ &= (\varepsilon \mid c \mid bc)(abc)^*(\varepsilon \mid a \mid ab) \mid b \end{aligned}$$

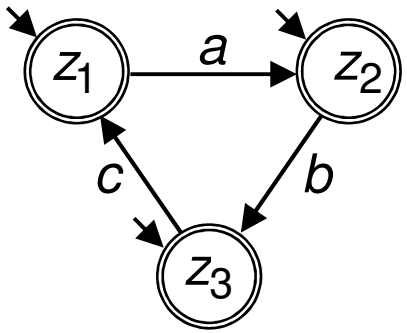
Büchi-Automaten und ω-Sprachen

Ein Automat *A* definiert **auch** eine sog. ω-**Sprache** $L_\omega(A)$ unendlicher Folgen;

A (obwohl unverändert) wird dann als **Büchi-Automat** bezeichnet:

Die Reisen werden unendlich lange, und zur ω-Sprache gehören („vom Büchi-Automaten **akzeptiert**“ werden) alle **Folgen** („unendlichen Reisetagebücher“), bei denen **mindestens ein Zielzustand unendlich oft** besucht wurde.

– **Formale Definition?** –



Welche ω-Sprache definiert der nebenstehende Büchi-Automat?

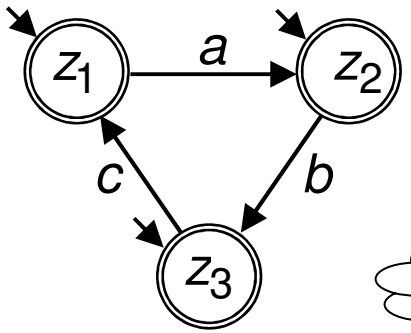
Wie kann ich ihn verändern,
ohne seine ω-Sprache zu verändern?

Büchi-Automaten und ω-Sprachen

Ein Automat *A* definiert **auch** eine sog. ω-**Sprache** $L_\omega(A)$ unendlicher Folgen; *A* (obwohl unverändert) wird dann als **Büchi-Automat** bezeichnet:

Die Reisen werden unendlich lange, und zur ω-Sprache gehören („vom Büchi-Automaten **akzeptiert**“ werden) alle **Folgen** („unendlichen Reisetagebücher“), bei denen **mindestens ein Zielzustand unendlich oft** besucht wurde.

– **Formale Definition?** –



Welche ω-Sprache definiert der nebenstehende Büchi-Automat?

$$L_\omega(A) = (\varepsilon \mid c \mid bc)abcabcabc\cdots = (\varepsilon \mid c \mid bc)(abc)^\omega$$

informell

„ω-regulärer Ausdruck“

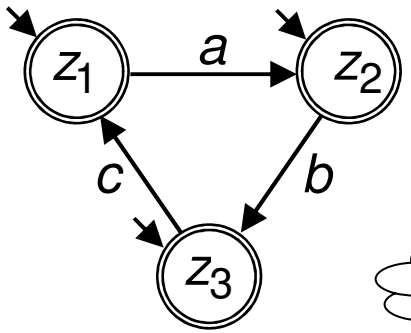
Wie kann ich ihn verändern,
ohne seine ω-Sprache zu verändern?

Büchi-Automaten und ω-Sprachen

Ein Automat *A* definiert **auch** eine sog. ω-**Sprache** $L_\omega(A)$ unendlicher Folgen; *A* (obwohl unverändert) wird dann als **Büchi-Automat** bezeichnet:

Die Reisen werden unendlich lange, und zur ω-Sprache gehören („vom Büchi-Automaten **akzeptiert**“ werden) alle **Folgen** („unendlichen Reisetagebücher“), bei denen **mindestens ein Zielzustand unendlich oft** besucht wurde.

– **Formale Definition?** –



Welche ω-Sprache definiert der nebenstehende Büchi-Automat?

$$L_\omega(A) = (\varepsilon \mid c \mid bc)abcabcabc\cdots = (\varepsilon \mid c \mid bc)(abc)^\omega$$

informell

„ω-regulärer Ausdruck“

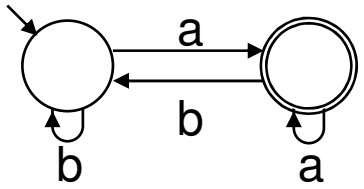
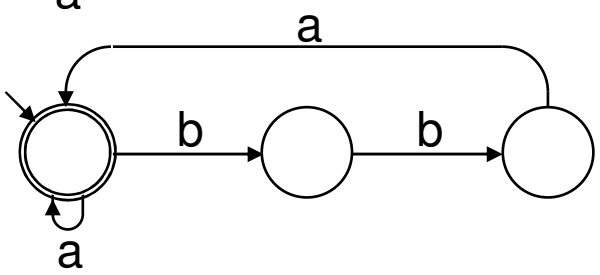
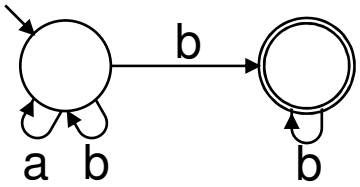
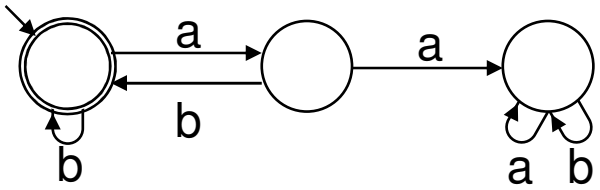
Wie kann ich ihn verändern, ohne seine ω-Sprache zu verändern?

z.B. einen oder zwei Zustände aus Z_{Ziel} streichen

Übung: Büchi-Automaten – weitere Beispiele

Alphabet = {a,b}

Ordnen Sie den Büchi-Automaten die richtigen ω-Sprachen zu.

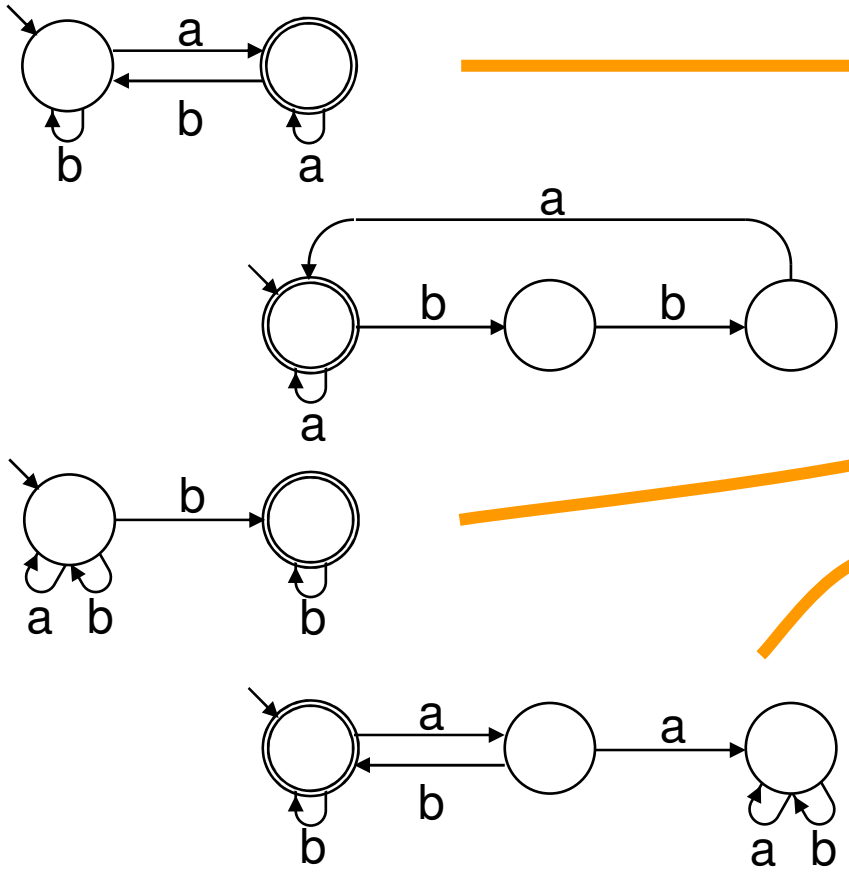
Büchi-Automat	**„Büchi-erkennbare“ ω-Sprache**
	unendlich viele a’s drin
	nur endlich viele a’s drin
	nie zwei a’s hintereinander (kein ...aa...)
	b’s nur zu zweit hintereinander (kein ...aba/bbb...)

Büchi-Automaten – weitere Beispiele

Alphabet = {a,b}

Ordnen Sie den Büchi-Automaten die richtigen ω-Sprachen zu.

Büchi-Automat **„Büchi-erkennbare“ ω-Sprache**



unendlich viele a’s drin

nur endlich viele a’s drin

nie zwei a’s hintereinander
(kein ...aa...)

b’s nur zu zweit hintereinander
(kein ...aba/bbb...)

PLTL-Formeln, ω-Sprachen und Büchi-Automaten

Sei AV_φ := Menge der in φ vorkommenden Aussagevariablen.

Jedes (die Formel **wahr** machende) **Modell** einer **PLTL-Formel** φ ist eine Folge $\pi = (\pi_0, \pi_1, \ldots)$, $\pi_i \subseteq AV_\varphi \subseteq AV$.

Wegen der Endlichkeit von AV_φ können wir die endliche Menge $\Sigma := \mathbf{P}(AV_\varphi)$ als ein **Alphabet** (mit etwas ungewöhnlichen Symbolen) betrachten!

Beispiel

$AV_\varphi = \{A, B, C\}$ → $\Sigma = \{ \varnothing, \{A\}, \{B\}, \{C\}, \{A,B\}, \{A,C\}, \{B,C\}, \{A,B,C\} \}$.

Mod(φ), die Menge aller Modelle von φ, ist dann eine **ω-Sprache** über Σ.

Satz: PLTL-Formel-Modelle werden von Büchi-Automaten akzeptiert.

Zu jeder PLTL-Formel φ über der Aussagevariablenmenge AV existiert ein Büchi-Automat A mit Alphabet $\Sigma = \mathbf{P}(AV)$, so dass **Mod(φ) = $L_\omega(A)$**

vgl. z.B. http://i12www.ira.uka.de/~pschmitt/FormSys/FormSys1112/skriptum.pdf

PLTL ←→ Büchi-Automat: Beispiel

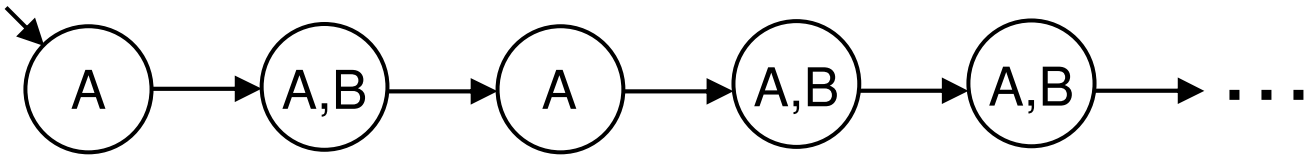
PLTL-Formel über {*A*,*B*}:

$A \wedge \neg B \wedge$
$G(\neg B \rightarrow XB) \wedge$
$G(B \rightarrow A) \wedge$
$G(B \rightarrow X$
$\quad ((A \wedge \neg B) \vee GB) \wedge$
FGB

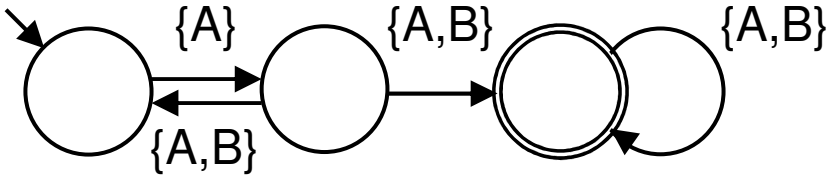
Wirkung auf die **Modelle** über {*A*,*B*}:

Die erste Situation ist {A} &
keine 2 hintereinander ohne B &
stets wo {B,…}, dort {A,B} &
stets folgt auf {B,…} sofort
{A} oder für immer {B,…} &
irgendwann kommt für immer {B,…}.

Modellbeispiel:



Büchi-Automat
für die Modelle:



Anwendung: Erfüllbarkeit, Allgemeingültigkeit

Satz (**Büchi-Entscheidbarkeit**)
Die Frage, ob für einen Büchi-Automaten A die Sprache der akzeptierten Wörter nicht leer ist, d.h. $L_\omega(A) \neq \emptyset$, ist **entscheidbar**.

Beweis siehe z.B. wie vorgehend

Korollar (**PLTL-Entscheidbarkeit**)
Erfüllbarkeit und **Allgemeingültigkeit** jeder PLTL-Formel φ sind **entscheidbar**.

Beweis:
Man konstruiert die Büchi-Automaten A und B mit $\mathrm{Mod}(\varphi) = L_\omega(A)$ und $\mathrm{Mod}(\neg\varphi) = L_\omega(B)$.
Nun ist φ erfüllbar $\Leftrightarrow L_\omega(A) \neq \emptyset$ und φ allgemeingültig $\Leftrightarrow L_\omega(B) = \emptyset$.

Erinnerung: Reguläre Ausdrücke

Die Menge der **regulären Ausdrücke** $Reg(\Sigma)$ über einem Alphabet Σ ist induktiv definiert:

- $\emptyset, \varepsilon \in Reg(\Sigma)$
- $\Sigma \subseteq Reg(\Sigma)$ (Zeichen "=" Wort der Länge 1)
- $p, q \in Reg(\Sigma) \Rightarrow p^*, (p|q), (pq) \in Reg(\Sigma)$.

Jeder reguläre Ausdruck *reg* definiert rekursiv eine **Sprache L(*reg*)**:

- $L(\emptyset) := \emptyset$
- $L(a) := \{a\}$ für alle $a \in \Sigma$
- $L(p^*) := (L(p))^*$
- $L((p|q)) := L(p) \cup L(q)$
- $L((pq)) := \{vw \mid v \in L(p) \wedge w \in L(q)\}$

Beispiel: L(a*bb*(aa*bb*)*) = L((a|b)*b) = Wörter aus a und b mit b am Ende.

Äußere Klammern können ausgelassen werden,
weitere Klammern bei Einführung von **Bindungsprioritäten** (z.B. * > ∘ > |),
noch weitere wegen **Assoziativität**.

Kleene vor Verkettung
vor Alternative

ω-reguläre Ausdrücke

Die Menge der ω**-regulären Ausdrücke** ω-$Reg(\Sigma)$ über einem Alphabet Σ ist induktiv definiert:

- $\emptyset \in \omega\text{-}Reg(\Sigma)$
- $p \in Reg(\Sigma) \wedge \varepsilon \notin L(p) \quad \Rightarrow \quad p^{\omega} \in \omega\text{-}Reg(\Sigma)$
- $p, q \in \omega\text{-}Reg(\Sigma) \quad \Rightarrow \quad (p+q) \in \omega\text{-}Reg(\Sigma)$
- $p \in Reg(\Sigma) \wedge q \in \omega\text{-}Reg(\Sigma) \quad \Rightarrow \quad (pq) \in \omega\text{-}Reg(\Sigma)$

Jeder ω-reguläre Ausdruck q definiert rekursiv eine **Sprache $L^{\omega}(q)$ unendlicher** Wörter:

- $L^{\omega}(\emptyset) := \emptyset$
- $L^{\omega}((p+q)) := L^{\omega}(p) \cup L^{\omega}(q)$
- $L^{\omega}(p^{\omega}) := \{v_1 v_2 \cdots \mid \forall i \geq 1 : v_i \in L(p)\}$
- $L^{\omega}((pq)) := \{vw \mid v \in L(p) \wedge w \in L^{\omega}(q)\}$

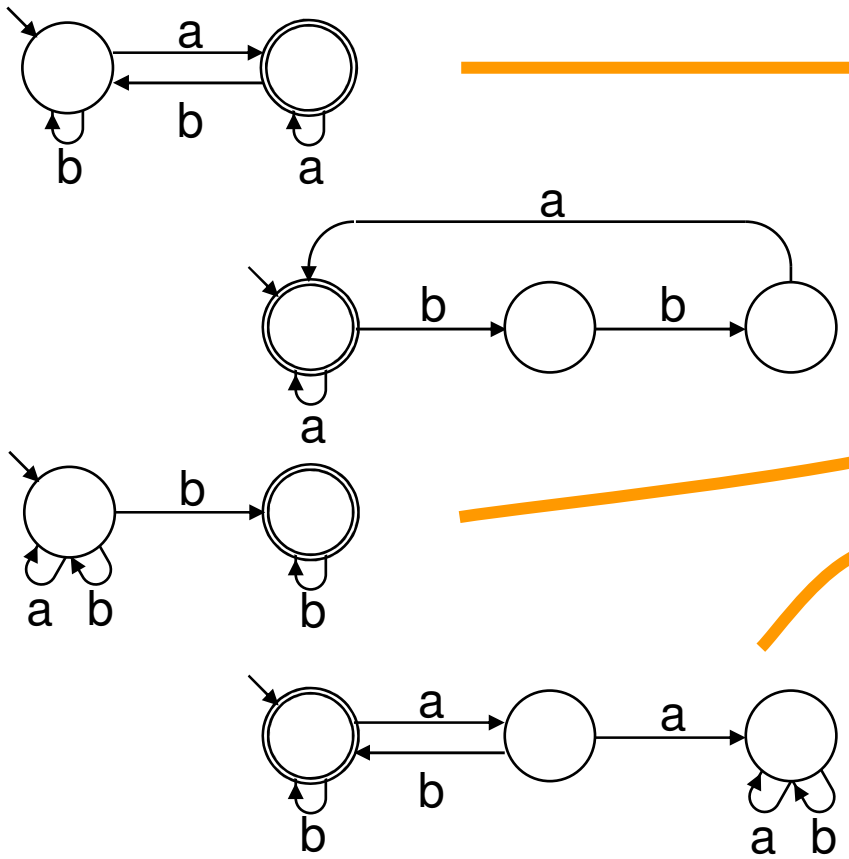
Büchi-Automaten und ω-reguläre Ausdrücke
„definieren dieselben Sprachen über $\Sigma = \mathbf{P}(AV)$,“
und daher sind auch PLTL-Formel-Modellmengen ω-regulär darstellbar.

Büchi-Automaten – weitere Beispiele

Alphabet = {a,b}

Büchi-Automaten – ω-Sprachen – ω-reguläre Ausdrücke

Büchi-Automat **„Büchi-erkennbare“ ω-Sprache**



unendlich viele a’s drin

nur endlich viele a’s drin

nie zwei a’s hintereinander
(kein ...aa...)

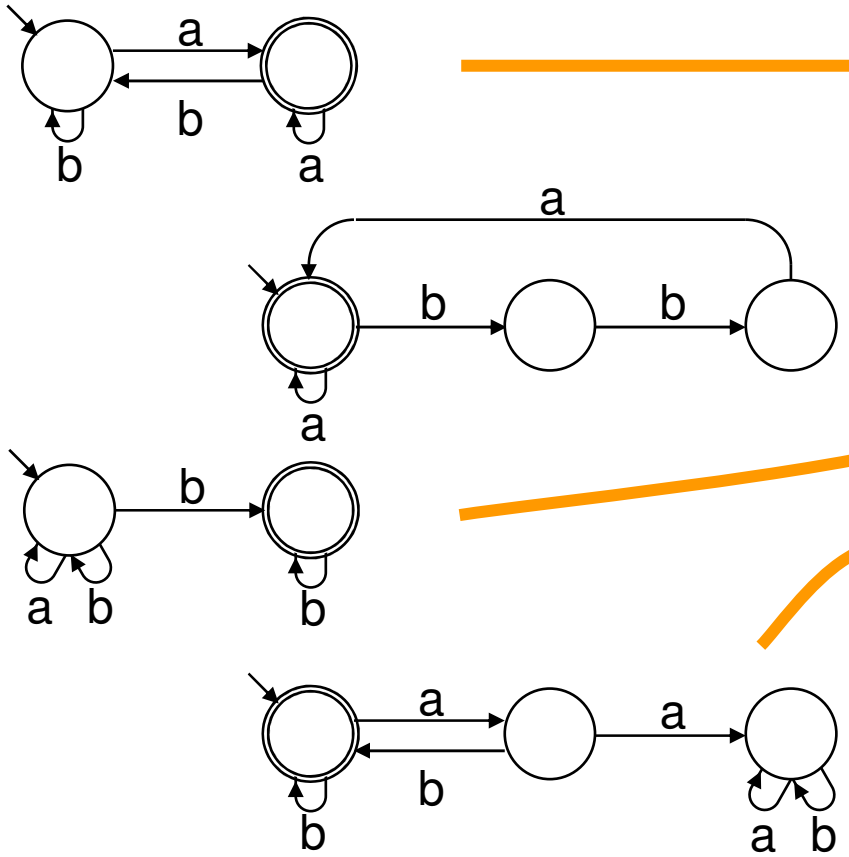
b’s nur zu zweit hintereinander
(kein ...aba/bbb...)

Büchi-Automaten – weitere Beispiele

Alphabet = {a,b}

Büchi-Automaten – ω-Sprachen – ω-reguläre Ausdrücke

Büchi-Automat **„Büchi-erkennbare“ ω-Sprache**



unendlich viele a’s drin

$(b^*a)^\omega$

nur endlich viele a’s drin

$(b^*a)^*b^\omega$, $(a+b)^*b^\omega$

nie zwei a’s hintereinander

(kein ...aa...)

$(b^*ab)^*(b^\omega|(b^*ab)^\omega)$, $(a+(\varnothing)^*)(b+ba)^\omega$

b’s nur zu zweit hintereinander

(kein ...aba/bbb...)

$(a|bba)^\omega$

PLTL mit einelementigen Belegungen

Es gibt Anwendungsbereiche, bei denen
jede Situation mit genau einer Aussagevariable belegt ist.
Mit $AV = \{A_1, \cdots, A_n\}$ entspräche das dem **Axiom** „$\Box$**XOR**$(A_1, \cdots, A_n)$“, d.h.

$$\Box[(A_1 \vee \cdots \vee A_n) \wedge (\neg(A_1 \wedge A_2)) \wedge (\neg(A_1 \wedge A_3)) \wedge \cdots \wedge (\neg(A_{n-1} \wedge A_n))]$$

Man beschreibt oft Systeme mittels möglicher **Aktionen** $Act = \{a_1, \cdots, a_n\}$,
die sequentiell beobachtet werden, z.B. die

Systembeobachtung = Aktionenfolge $a_1 a_2 a_3 a_1$ ...

$A_i \cong$ „a_i ist als letztes geschehen“ (anfangs *nil* $\cong$ noch keine Aktion)

→ in jeder Situation ist genau eine Aussagevariable wahr, z.B.

nil A_1 A_2 A_3 A_1 $\cdots$ für a_1 a_2 a_3 a_1 $\cdots$

Dann brauchen wir auch keine Potenzmenge mehr. ☺

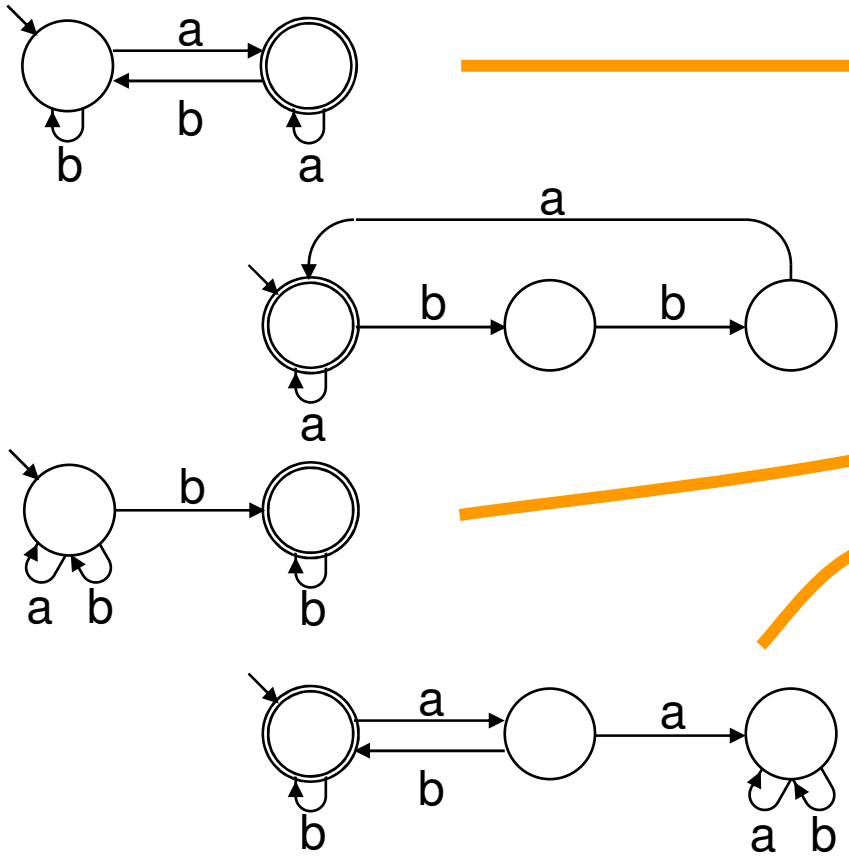
Büchi-Automaten – weitere Beispiele

& „einelementige“ PLT-Formeln?

Alphabet = {a,b}

Büchi-Automaten – ω-Sprachen – ω-reguläre Ausdrücke

Büchi-Automat **„Büchi-erkennbare“ ω-Sprache**



unendlich viele a’s drin

$(b^*a)^\omega$

nur endlich viele a’s drin

$(b^*a)^*b^\omega$, $(a+b)^*b^\omega$

nie zwei a’s hintereinander

(kein ...aa...)

$(b^*ab)^*(b^\omega|(b^*ab)^\omega)$, $(a+(\varnothing)^*)(b+ba)^\omega$

b’s nur zu zweit hintereinander

(kein ...aba/bbb...)

$(a|bba)^\omega$

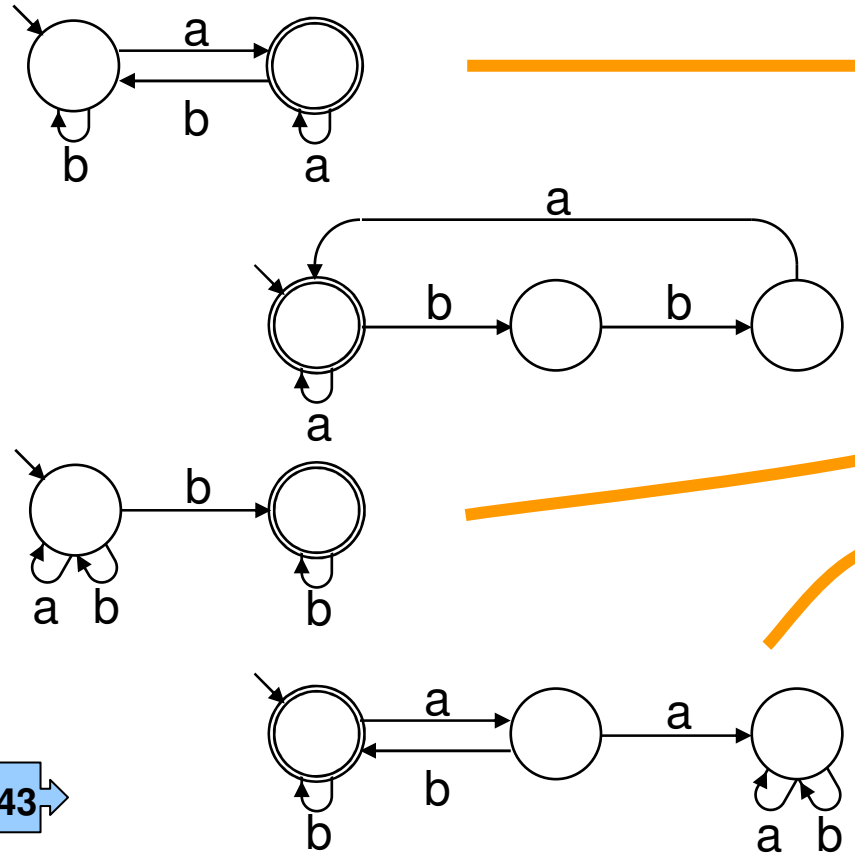
Büchi-Automaten – weitere Beispiele

Alphabet = {a,b}

& „einelementige“ PLT-Formeln

Büchi-Automaten – ω-Sprachen – ω-reguläre Ausdrücke

Büchi-Automat | **„Büchi-erkennbare“ ω-Sprache**



unendlich viele a’s drin

GFa , ¬FGb (b*a)$^\omega$

nur endlich viele a’s drin

¬GFa, FGb (b*a)*b$^\omega$, (a+b)*b$^\omega$

nie zwei a’s hintereinander

G(a→¬Xa), ¬F(a+Xa) (kein ...aa...)

(b*ab)*(b$^\omega$ | (b*ab)$^\omega$), (a+(∅)*)(b+ba)$^\omega$

b’s nur zu zweit hintereinander

(kein ...aba/bbb...)

¬F(a∧Xb∧XXa)∧¬F(b∧Xb∧XXb) (a|bba)$^\omega$

Ü43

PLTL-Kritik: Falsifizierbarkeitsproblem

Soll man **Systemeigenschaften spezifizieren**,
deren **Verletzung nie festzustellen** ist –
weder direkt noch indirekt? (→ K. Popper)

Beispiel: Black Box, zeigt ab jetzt jede Sekunde eine Zahl: 0 oder 1.
Beobachtbar: (beliebig lange aber endliche) **Anfangsstücke**!

Wunscheigenschaft: **abwechs. 0 und 1!** PLTL: $\Box[(0 \rightarrow X1) \wedge (1 \rightarrow X0)]$

Beobachtung dass **einwandfrei**: **unmöglich** („meta-☺“ erst im ∞)

Beobachtung dass **fehlerhaft**: **möglich** z.B. 00 ☹,

aber **zeitlich nicht einzugrenzen**: 10101010101010101010 😐,

Wunscheigenschaft: **irgendwann 1!** PLTL: $\Diamond 1$

Beobachtung dass **einwandfrei**: **möglich** z.B. 00001 ☺,

aber **zeitlich nicht einzugrenzen**: 00000000000000000000 😐,

Beobachtung dass **fehlerhaft**: **unmöglich** („meta-☹“ erst im ∞),

→ http://www.bernd-baumgarten.de/Dru/PostDruA.pdf, S.1-11